IN THE CLAIMS

Please amend the claims as follows:

Claims 1-5 (Canceled)

6. (Presently Amended) A method for achieving crypto-synchronization in a packet data communication system, the packet data communication system comprising a transmitter and a receiver, said transmitter and said receiver each having cryptographic security capabilities, comprising:

generating data frames at a predetermined rate in a transmitter;

incrementing a state vector at said predetermined rate;

providing said state vector to an encryption module;

generating a codebook from said encryption module, using at least said state vector, said codebook for encrypting at least one of said data frames;

detecting a delay in transmitting said data frames;

dropping one or more of said frames; and

disabling said state vector from incrementing for each of said data frames being dropped, wherein said dropping one or more of said data frames comprises:

determining a communication channel latency; and

dropping said data frames at a variable rate in accordance with said communication channel latency, and

~~The method of claim 5~~ wherein said dropping said data frames at a variable rate comprises:

decreasing said rate if said communication channel latency falls below at least one predetermined threshold; and

increasing said rate if said communication channel latency exceeds at least one other predetermined threshold.

7. (Presently Amended) A method for achieving crypto-synchronization in a packet data communication system, the packet data communication system comprising a transmitter and a receiver, said transmitter and said receiver each having cryptographic security capabilities, comprising:

generating data frames at a predetermined rate in a transmitter;

incrementing a state vector at said predetermined rate;

providing said state vector to an encryption module;

generating a codebook from said encryption module, using at least said state vector, said codebook for encrypting at least one of said data frames;

detecting a delay in transmitting said data frames;

dropping one or more of said frames; and

disabling said state vector from incrementing for each of said data frames being dropped,

~~The method of claim 1~~ wherein said dropping said data frames comprises:

determining a communication channel latency;

dropping said data frames at a first predetermined fixed rate if said communication channel latency falls below a predetermined threshold; and

dropping said data frames at a second predetermined fixed rate if said communication channel latency exceeds said predetermined threshold.

8. (Canceled)

9. (Presently Amended) A method for achieving crypto-synchronization in a packet data communication system, the packet data communication system comprising a transmitter and a receiver, said transmitter and said receiver each having cryptographic security capabilities, comprising:

generating data frames at a predetermined rate in a transmitter;

incrementing a state vector at said predetermined rate;

providing said state vector to an encryption module;

generating a codebook from said encryption module, using at least said state vector, said codebook for encrypting at least one of said data frames;

detecting a delay in transmitting said data frames;

dropping one or more of said frames;

disabling said state vector from incrementing for each of said data frames being dropped, wherein said dropping one or more of said data frames comprises:

determining a communication channel latency; and

dropping each of said data frames having an encoded rate equal to a first encoding rate if said communication channel latency exceeds a predetermined threshold; and ~~The method of claim 8, further comprising~~

dropping each of said data frames having an encoded rate equal to said first encoding rate and a second encoding rate if said communication channel latency exceeds a second predetermined threshold.

Claims 10-11 (Canceled)

12. (Presently Amended) A method for achieving crypto-synchronization in a packet data communication system, the packet data communication system comprising a transmitter and a receiver, said transmitter and said receiver each having cryptographic security capabilities, comprising:

receiving data frames at a receiver;

storing said data frames in sequence in a queue;

providing said stored data frames, in sequence, to a decryption module;

incrementing a state vector at a predetermined rate;

providing said state vector to the decryption module;

generating a codebook from said decryption module, using at least said state vector, said codebook for decrypting at least one of said data frames;

detecting that the data frames in the queue exceed a limit;

dropping one or more of said data frames in said queue; and

adjusting said state vector for each of said one or more data frames that are dropped, wherein said adjusting said state vector comprises:

determining a number of dropped data frames; and

advancing said state vector in proportion to said number of dropped frames, and

~~The method of claim 11~~ wherein said advancing said state vector comprises advancing said state vector by a value of one for each of said one or more dropped frames.

Claims 13-15 (Canceled)

16. (Presently Amended) A method for achieving crypto-synchronization in a packet data communication system, the packet data communication system comprising a transmitter and a receiver, said transmitter and said receiver each having cryptographic security capabilities, comprising:

receiving data frames at a receiver;

storing said data frames in sequence in a queue;

providing said stored data frames, in sequence, to a decryption module;

incrementing a state vector at a predetermined rate;

providing said state vector to the decryption module;

generating a codebook from said decryption module, using at least said state vector, said codebook for decrypting at least one of said data frames;

detecting that the data frames in the queue exceed a limit;

dropping one or more of said data frames in said queue; and

adjusting said state vector for each of said one or more data frames that are dropped, wherein said dropping one or more of said data frames comprises:

determining a communication channel latency; and

dropping said one or more data frames at a variable rate in accordance with said communication channel latency, and

~~The method of claim 15~~ wherein said dropping said one or more of said data frames at a variable rate comprises:

decreasing said rate if said communication channel latency falls below at least one predetermined threshold; and

increasing said rate if said communication channel latency exceeds at least one other predetermined threshold.

17. (Presently Amended) A method for achieving crypto-synchronization in a packet data communication system, the packet data communication system comprising a transmitter and a receiver, said transmitter and said receiver each having cryptographic security capabilities, comprising:

receiving data frames at a receiver;

storing said data frames in sequence in a queue;

providing said stored data frames, in sequence, to a decryption module;

incrementing a state vector at a predetermined rate;

providing said state vector to the decryption module;

generating a codebook from said decryption module, using at least said state vector, said codebook for decrypting at least one of said data frames;

detecting that the data frames in the queue exceed a limit;

dropping one or more of said data frames in said queue; and

adjusting said state vector for each of said one or more data frames that are dropped

~~The method of claim 10~~ wherein said dropping said one or more of said data frames comprises:

determining a communication channel latency;

dropping said data frames at a first predetermined fixed rate if said communication channel latency falls below a predetermined threshold; and

dropping said data frames at a second predetermined fixed rate if said communication channel latency exceeds said predetermined threshold.

18. (Canceled)

19. (Presently Amended) A method for achieving crypto-synchronization in a packet data communication system, the packet data communication system comprising a transmitter and a receiver, said transmitter and said receiver each having cryptographic security capabilities, comprising:

receiving data frames at a receiver;

storing said data frames in sequence in a queue;

providing said stored data frames, in sequence, to a decryption module;

incrementing a state vector at a predetermined rate;

providing said state vector to the decryption module;

generating a codebook from said decryption module, using at least said state vector, said codebook for decrypting at least one of said data frames;

detecting that the data frames in the queue exceed a limit;

dropping one or more of said data frames in said queue;

adjusting said state vector for each of said one or more data frames that are dropped, wherein said dropping one or more of said data frames comprises:

determining a communication channel latency; and

dropping each of said data frames having an encoded rate equal to a first encoding rate if said communication channel latency exceeds a predetermined threshold, and

~~The method of claim 18, further comprising~~ dropping one or more of said data frames having an encoded rate equal to said first encoding rate and a second encoding rate if said communication channel latency exceeds a second predetermined threshold.

20. (Canceled)

21. (Presently Amended) A method for achieving crypto-synchronization in a packet data communication system, the packet data communication system comprising a transmitter and a receiver, said transmitter and said receiver each having cryptographic security capabilities, comprising:

receiving data frames at a receiver;

storing said data frames in a queue;

providing at least one of said data frames from said queue to a decryption module if available in said queue;

providing a state vector to said decryption module, said state vector incremented at a predetermined rate;

generating a codebook from said decryption module, using at least said state vector, said codebook for decrypting at least one of said data frames;

detecting that no data frame is available in said queue for decryption; and

disabling said state vector when no data frame is available for decryption in said queue, ~~The method of claim 20,~~ wherein said disabling said state vector comprises:

determining that none of said data frames are available for decryption in said queue;

disabling said state vector;

determining that at least one of said data frames is available for decryption in said queue;

enabling said state vector; and

incrementing said state vector by a value of one.

Claims 22-24 (Canceled)

25. (Presently Amended) A transmitter for achieving crypto-synchronization in a packet data communication system, the packet data communication system comprising said transmitter and a receiver, said transmitter and said receiver each having cryptographic security capabilities, said transmitter comprising:

means for generating data frames at a predetermined rate;

means for generating a state vector, said state vector incremented at said predetermined rate;

an encryption module adapted to generate a codebook from at least said state vector, said codebook for encrypting at least one of said data frames; and

a processor adapted to detect a delay in transmitting said data frames, to drop one or more of said data frames, and to disable said state vector for each of said data frames that are dropped, wherein said data frames are dropped at a variable rate, and

~~The apparatus of claim 24,~~ wherein:

said processor is further for determining a communication channel latency;

said data frames are dropped at a decreased rate if said communication channel latency exceeds at least one predetermined threshold; and

said data frames are dropped at an increased rate if said communication channel latency falls below at least one other predetermined threshold.

Claims 26-27 (Canceled)

28. (Presently Amended) A transmitter for achieving crypto-synchronization in a packet data communication system, the packet data communication system comprising said transmitter and a receiver, said transmitter and said receiver each having cryptographic security capabilities, said transmitter comprising:

means for generating data frames at a predetermined rate;

means for generating a state vector, said state vector incremented at said predetermined rate;

an encryption module adapted to generate a codebook from at least said state vector, said codebook for encrypting at least one of said data frames; and

a processor adapted to detect a delay in transmitting said data frames, to drop one or more of said data frames, and to disable said state vector for each of said data frames that are dropped, wherein said processor is further for determining a communication channel latency, and for dropping each of said data frames having an encoded rate equal to a first encoding rate if said communication channel latency exceeds a predetermined threshold, and

~~The apparatus of claim 27,~~ wherein said processor is further for dropping each of said data frames having an encoded rate equal to said first encoding rate and a second encoding rate if said communication channel latency exceeds a second predetermined threshold.

Claims 29-31 (Canceled)

32. (Presently Amended) A receiver for achieving crypto-synchronization in a packet data communication system, the packet data communication system comprising a transmitter and said receiver, said transmitter and said receiver each having cryptographic security capabilities, said receiver comprising:

means for receiving data frames;

a queue adapted to store said data frames;

means for generating a state vector, said state vector incremented at a predetermined rate;

a decryption module adapted to generate a codebook from at least said state vector, said codebook for decrypting at least one of said data frames; and

a processor adapted to detect a delay in decryption of said data frames, to drop one or more of said data frames in said queue, and to adjust said state vector for each of said data frames that are dropped,

wherein said processor adjusts said state vector by determining a number of dropped data frames and advancing said state vector in proportion to said number of dropped frames, and

~~The receiver of claim 31~~ wherein said state vector is advanced by a value of one for each of said dropped data frames.

Claims 33-34 (Canceled)

35. (Presently Amended) A receiver for achieving crypto-synchronization in a packet data communication system, the packet data communication system comprising a transmitter and said receiver, said transmitter and said receiver each having cryptographic security capabilities, said receiver comprising:

means for receiving data frames;

a queue adapted to store said data frames;

means for generating a state vector, said state vector incremented at a predetermined rate;

a decryption module adapted to generate a codebook from at least said state vector, said codebook for decrypting at least one of said data frames; and

a processor adapted to detect a delay in decryption of said data frames, to drop one or more of said data frames in said queue, and to adjust said state vector for each of said data frames that are dropped,

wherein said processor is further for determining a communication channel latency and dropping said one or more data frames at a variable rate in accordance with said communication channel latency, and

~~The receiver of claim 34~~ wherein:

said processor decreases said rate if said communication channel latency falls below at least one predetermined threshold; and

said processor increases said rate if said communication channel latency exceeds at least one other predetermined threshold.

36. (Presently Amended) A receiver for achieving crypto-synchronization in a packet data communication system, the packet data communication system comprising a transmitter and said receiver, said transmitter and said receiver each having cryptographic security capabilities, said receiver comprising:

means for receiving data frames;

a queue adapted to store said data frames;

means for generating a state vector, said state vector incremented at a predetermined rate;

a decryption module adapted to generate a codebook from at least said state vector, said codebook for decrypting at least one of said data frames; and

a processor adapted to detect a delay in decryption of said data frames, to drop one or more of said data frames in said queue, and to adjust said state vector for each of said data frames that are dropped,

~~The receiver of claim 30~~ wherein said processor is further for determining a communication channel latency; and

dropping said one or more data frames at a first predetermined fixed rate if said communication channel latency falls below a predetermined threshold; and

dropping said one or more data frames at a second predetermined fixed rate if said communication channel latency exceeds said predetermined threshold.

37. (Canceled)

38. (Presently Amended) A receiver for achieving crypto-synchronization in a packet data communication system, the packet data communication system comprising a transmitter and said receiver, said transmitter and said receiver each having cryptographic security capabilities, said receiver comprising:

means for receiving data frames;

a queue adapted to store said data frames;

means for generating a state vector, said state vector incremented at a predetermined rate;

a decryption module adapted to generate a codebook from at least said state vector, said codebook for decrypting at least one of said data frames; and

a processor adapted to detect a delay in decryption of said data frames, to drop one or more of said data frames in said queue, and to adjust said state vector for each of said data frames that are dropped,

wherein said processor is further for determining a communication channel latency; and

dropping each of said one or more data frames having an encoded rate equal to a first encoding rate if said communication channel latency exceeds a predetermined threshold, and

~~The receiver of claim 37~~ wherein said processor drops said one or more data frames having an encoded rate equal to said first encoding rate and a second encoding rate if said communication channel latency exceeds a second predetermined threshold.

Claims 39-40 (Canceled)